

REMARKS

Claims 1-37 are pending.

Enablement Requirement

Applicants respectfully submit that “pipeline” is a term of art understood by one of ordinary skill in the art. The Examiner is reminded that the scope of the claims is determined from the point of view of one of ordinary skill in the art. If the Examiner is stating for the record that one of ordinary skill in the art would not understand the term “pipeline” or “pipeline stage” or “single pipeline stage”, then the Examiner is requested to so state this for the record.

It is however noted that even a document cited by the Examiner uses the term “pipeline”.

It is respectfully requested that the enablement rejection be withdrawn with respect to claim 2.

Indefiniteness

As mentioned before, the term “single pipeline stage decryption” is understood by one of ordinary skill in the art. There is no indefiniteness. The standard whether one of ordinary skill in the art would understand the term. Since “pipeline” was even used in one of the documents cited by the Examiner, it may be deduced that one of ordinary skill in the art would understand “single pipeline stage decryption”.

With respect to the term “substantially” as recited in claim 17, the Office Action alleges that it is an indefinite term “because it is unclear whether the limitations following the phrase are part of the claimed invention” and cites M.P.E.P. § 2173.05(d). M.P.E.P. § 2173.05(d) is not a relevant citation since it relates to the phrases “for example” and “such as”. Instead, the Examiner should look at M.P.E.P. 2173.05(b)(D) which states that “substantially” is a definite term.

Applicants have amended claim 34 to further clarify the subject matter therein.

It is respectfully requested that the indefiniteness rejection be withdrawn with respect to claims 2, 17 and 34.

Claim Objections

Claims 7, 10 and 22 recite subject matter that is not expressly recited in the parent claim, namely, claim 1. Thus, the objection under 37 C.F.R. § 1.75(c) is unfounded.

For example, claim 10 recites, in part, “two-bit adders”. Claim 1 does not recite “two-bit adders”. There can be no doubt that claim 10 is narrower in scope than claim 1. It is narrower because it adds further limitations to the recitations of claim 1.

Claim 22 recites, in part, that the decryptor is adapted to receive encrypted data from the memory. Claim 1 recites only that the processor is coupled to the memory. These elements in claim 22 further clarify the subject matter recited in claim 1.

A similar argument can be made with respect to claim 7.

It is respectfully requested that the claim objections be withdrawn with respect to claims 7, 10 and 22.

Anticipation Rejection Based on Richard

Claims 1 and 2 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,004,089 (“Richard”). Applicants respectfully traverse the rejection.

Claim 1 recites, in part, “the decryptor being adapted to variably bit roll the encrypted data”.

The Office Action alleges that Richard at col. 1, lines 61-65 describes at least these elements as set forth in claim 1. Applicants respectfully disagree. The cited text does not mention or describe bit rolling at all. Instead, Richard at col. 1, lines 61-65 describes a process of generating a long, non-linear pseudo-random sequence bit signal. As Richard at col. 42-44 describes, the long, non-linear pseudo-random sequence bit signal is “modulo-two added” to clear text. Respectfully, this is not bit rolling.

It is respectfully requested that the rejection under 35 U.S.C. § 102(b) based on Richard be withdrawn with respect to claim 1 and its rejected dependent claim (i.e., claim 2).

Anticipation Rejection Based on Luyster

Claims 1-37 stand rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Publication No. 2001 0038693 A1 (“Luyster”). Applicants respectfully traverse the rejection.

Claims 25 and 20

Claim 25 recites, in part, “the processor comprising a decryptor that decrypts the encrypted data and decrypts a word of the encrypted data *in a single cycle*”. The Office Action alleges that Luyster at paragraph [95] describes at least these elements as set forth in claim 25. Applicants respectfully disagree.

Luyster describes an iterative process in which a plurality of “rounds” are required to encrypt data. For example, FIG. 3 is “an algorithmic flow chart for one round of the cryptographic system”. Luyster at paragraph [0123]. Luyster at paragraph [0124] refers to the “iterative enciphering process”. Luyster at paragraph [0008] refers to “[b]lock ciphers ... have many rounds”.

Thus, Luyster does not decrypt in a single cycle as set forth in claim 25.

For at least the above reasons, it is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be withdrawn with respect to claim 25.

In addition, claim 20 recites that “the decryptor decrypts a word of the encrypted data in a single cycle”. For at least similar reasons stated with respect to claim 25, it is believed that claim 20 is also patentable over Luyster.

It is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be withdrawn with respect to claim 20.

Claims 24 and 19

Claim 24 recites, in part, “the processor comprising a decryptor that decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor”.

The Office Action alleges that Luyster at paragraph [0227] describes at least these elements as set forth in claim 24. Applicants respectfully disagree. Luyster at paragraph [0227] is focused on just a small part of the entire process of encryption in Luyster. In fact, as discussed with respect to

U.S. Application No. 10/695,008, filed October 28, 2003

Amendment dated March 7, 2007

In Response to Office Action of December 7, 2006

claim 25, Luyster describes an encryption process that is iterative and requires a plurality of “rounds”. Therefore, Luyster does not describe a decryptor that decrypts without adding enough gate delays to exceed a clock cycle budget of the processor.

It is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be withdrawn with respect to claim 24.

In addition, claim 19 recites that “the decryptor does not add enough gate delays to exceed a clock cycle budget of the processor”. For at least similar reasons stated with respect to claim 24, it is believed that claim 19 is also patentable over Luyster.

It is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be withdrawn with respect to claim 19.

Claims 1-22

As amended to expedite prosecution, claim 1 recites, in part, “the decryptor being adapted to variably bit roll the encrypted data based on at least a data address”. Applicants respectfully submit that Luyster does not describe at least these elements as set forth in claim 1.

Claim 3 previously recited, in part, “wherein the decryptor comprises a bit roller that rotates data in one or more roll regions of the incoming data *based on an address* related to the received encrypted data and a key related to the first key”. The Office Action alleged that at least these elements were described in Luyster at paragraphs [0138] and [0106]. Applicants respectfully disagree that Luyster describes a bit roller that rotates data based on an address related to the received encrypted data.

Accordingly, Applicants have added “based on at least a data address” to claim 1. It is believed that Luyster at paragraphs [0138] and [0106] do not describe “the decryptor being adapted to variably bit roll the encrypted data based on at least a data address” as set forth in claim 1.

It is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be withdrawn with respect to claim 1 and its rejected dependent claims (i.e., claims 2-22).

Claims 30-37

Claim 30 recites, in part, “variably rolling data information based on a first key and an address related to the data information”.

The Office Action alleges that Luyster at paragraphs [0138] and [0106] describes at least these elements. Applicants respectfully disagree.

As described above with respect to claims 1 and 3, Luyster does not describe variably rolling data information based on an address.

It is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be withdrawn with respect to claim 30 and its rejected dependent claims (i.e., claims 31-37).

Claims 26-29

As amended to expedite prosecution, claim 26 recites, in part, “the processor being adapted to variably bit roll encrypted data based on at least a data address”.

As described above, Luyster does not describe a processor that is adapted to variably bit roll encrypted data based on at least a data address.

It is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be withdrawn with respect to claim 26 and its rejected dependent claims (i.e., claims 27-29).

Claim 23

As amended to expedite prosecution, claim 23 recites, in part, “a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline, wherein decryptor comprises a variable bit roller that variably bit rolls encrypted data based on at least a data address, and wherein the decryptor decrypts a word of the encrypted data in a single cycle”.

Although Applicants are doubtful as to Luyster’s alleged description of “a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline”, in order to expedite prosecution, Applicants have amended claim 23 to include elements that, in view of the above discussions, Applicants do not believe are described in Luyster.

It is respectfully requested that rejection under 35 U.S.C. § 102(b) based on Luyster be

U.S. Application No. 10/695,008, filed October 28, 2003
Amendment dated March 7, 2007
In Response to Office Action of December 7, 2006

withdrawn with respect to claim 23.


Conclusion

In view of at least the foregoing, it is respectfully submitted that the pending claims 1-37 are in condition for allowance. Should anything remain in order to place the present application in condition for allowance, the Examiner is kindly invited to contact the undersigned at the below-listed telephone number.

The Commissioner is hereby authorized to charge additional fees or credit overpayments to the deposit account of McAndrews, Held & Malloy, Account No. 13-0017.

Date: March 7, 2007

Respectfully submitted,



Michael T. Cruz
Reg. No. 44,636

McANDREWS, HELD & MALLOY, LTD.
500 West Madison Street, Suite 3400
Chicago, Illinois 60661
Telephone: (312) 775-8084
Facsimile: (312) 775-8100